
**Personnel Administration Office
Alberta Security Screening Directive
Privacy Impact Assessment**

January, 2003

**Prepared by:
Information and Privacy Office
Alberta Human Resources and Employment**

**In consultation with:
Human Resource Policy and Consulting
Personnel Administration Office**



EXECUTIVE SUMMARY

The Alberta Security Screening Directive is intended to strengthen the due diligence process with respect to the appointment or reclassification of employees into certain designated positions. Individuals who are hired to specified positions will have undergone a screening that not only reviews their employment and reference information as is currently in place, but will also allow for the review and identification of any potential concerns through criminal records checks, and/or financial management risk indicators, and vulnerability risk indicators.

In addition, current employees in certain specified positions will have the opportunity to voluntarily complete the screening.

The authority for the collection and use of the personal information as indicated stems from the Public Service Act, the Government Organization Act, and the Freedom of Information and Protection of Privacy Act. The Personnel Administration Office is charged with the responsibility of implementing the Directive and coordinating related human resource programs and activities across the various Ministries, on behalf of the Government of Alberta, as one employer.

Personal information that is collected through this process will only be used for purposes outlined. It will be handled in a manner that respects the sensitivity and the privacy concerns of the individuals to whom the information pertains.

Table of Contents

EXECUTIVE SUMMARY	2
1.0 Description of the Alberta Security Screening Directive	5
1.1 Responsible Public Bodies	5
1.2 Responsible Business Area	5
1.3 Contact Person.....	6
1.4 Background.....	6
1.4.1 Role of the Personnel Administration Office (PAO)	6
1.4.2 Intent of the Alberta Security Screening Directive	7
1.5 Current Situation.....	8
1.5.1 Limitations of Current Security Screening Processes	8
1.5.2 Implications of the Directive on Current Security Screening Processes	8
1.6 Scope of the Alberta Security Screening Directive.....	9
1.6.1 Criminal Records Check (Level 1 & 2)	10
1.6.2 Financial Management Risk Indicator Check (Level 2 only)	10
1.6.3 Vulnerability Risk Indicator Screening (Level 2 only)	11
1.7 Benefits.....	11
1.8 Timing	12
2.0 Personal Information Collected, Used and Disclosed.....	13
2.1 Personal Information Collected	13
2.2 Information Flows	14
2.3 Information Users	17
2.3.1 The Individual's Ministry	17
2.3.2 Role of Executive Search, PAO	18
2.3.3 Role of Security Operations, Alberta Solicitor General	18
2.3.4 Role of the PAO	19
3.0 Protection of Personal Information Analysis.....	20
3.1 Collection of Personal Information	20
3.1.1 Authority of PSC to Set Personnel Policy	20
3.1.2 Application of Directive for New Hires and Appointments	21
3.1.3 Application of Directive to Current Employees	22
3.1.4 Authority of Deputy Ministers to Manage Personnel Activities	23
3.1.5 Authority to Collect Personal Information	24
3.2 Manner of Collection of Personal Information	25
3.3 Accuracy and Retention	26
3.3.1 Accuracy	26
3.3.2 Records Retention	27
3.4 Right to Request Correction of Personal Information	28
3.5 Protection of Personal Information.....	28
3.5.1 Security Provisions for Transmittal and Storage of Personal Information	29
3.6 Use of Personal Information.....	30
3.7 Disclosure of Personal Information	30
3.8 Disclosure for Research or Statistical Purposes.....	31
4.0 Potential Privacy Impacts	32
4.1 Potential Privacy Impacts.....	32
4.1.2 Conclusion	32
5.0 APPENDIX 1	33

5.1	Alberta Security Screening Directive.....	33
6.0	APPENDIX 2	36
6.1	Security Screening Process for Designated Future Employees.....	36
6.2	Security Screening Process for Designated Current Employees	39
7.0	APPENDIX 3	42
7.1	Instruction Sheet for Current Employees.....	43
7.2	Sample Release of Information Consent Form	44
7.3	Sample Release of Information Consent Form	45
7.4	Checklist Form	46
8.0	APPENDIX 4	47
8.1	Edmonton Police Service Security Screening Check.....	47
9.0	APPENDIX 5	48
9.1	Alberta Financial Risk Management Indicator Screening	48
9.2	Financial Management Risk Indicator Report Form	49
10.0	APPENDIX 6	50
10.1	Alberta Enhanced Security Screening Instructions.....	50
10.2	Alberta Enhanced Security Screening Form.....	50

1.0 DESCRIPTION OF THE ALBERTA SECURITY SCREENING DIRECTIVE

The Alberta Security Screening Directive, and its implementation, are the focus of this Privacy Impact Assessment (PIA).

For the purpose of this document "security screening" is the general term used to describe Criminal Records Checks and/or Financial Management Risk Indicator Screenings and/or Vulnerability Risk Indicator Screenings. Appendix 1 is the Alberta Security Screening Directive (referred to as the Directive in this report).

1.1 Responsible Public Bodies

The Personnel Administration Office (PAO) is responsible, on behalf of the Government of Alberta, for developing, implementing and maintaining the Directive.

Every Ministry, Board, Commission, or other entity under the Public Service Act is subject to this Directive and is responsible for complying with this Directive.

The process of implementing and maintaining the activities required under the directive will be one that is coordinated by PAO. As one employer, Human Resources is an integrated service¹ and program that ensures consistency across the Government of Alberta.

The security screening processes are described in Appendix 2.

1.2 Responsible Business Area

Staffing and Executive Search are responsible for coordinating and managing the Directive and associated processes.

¹ Integrated Service as referred to under s. 40(1)(i) of the *Freedom of Information and Protection of Privacy Act*

1.3 Contact Person

The following official can answer questions about the type of personal information collected and handled under the Directive for the purposes of this PIA:

Executive Director
Human Resource Policy and Consulting Services
Personnel Administration Office
6th Floor Peace Hills Trust Building, 10011-109 Street
Edmonton, Alberta T5J3S8
Phone: (780) 408-8400

1.4 Background

1.4.1 Role of the Personnel Administration Office (PAO)

The Personnel Administration Office (PAO) is the corporate human resources arm of the Alberta government. PAO establishes policy frameworks to support departments in achieving their business plan goals. PAO also works with departments to achieve cross-ministry human resource goals. Human resource directives are one tool that PAO utilizes to this end.

Human resource directives set out the general entitlements, benefits, authorities and requirements that apply in the administration of the employer's human resource program in Alberta government organizations under the *Public Service Act*. The purpose of a directive is to:

- Provide direction in the day-to-day administration of government human resources
- Provide a framework that encourages consistency and continuity in the administration of government human resources
- Provide degrees of flexibility to departments in addressing human resources issues
- Provide examples of standardized forms and other tools for departments to use and modify as required.

Every Ministry, Board, Commission, and any other entity subject to these directives is responsible for compliance (see sections 3.1.1 to 3.1.4 for a description of the legislative authority that exists between PAO and ministries).

Section 6(1)(c) of the Public Service Act provides the Public Service Commissioner with the general authority to:

(c) *advise and assist departments in the conduct of departmental personnel activities [emphasis added];*

This authorizes and supports the creation of a personnel, or human resources administration program within the Government of Alberta. In addition, individual Ministers are responsible for the ongoing personnel activity or program within their Ministries.

1.4.2 Intent of the Alberta Security Screening Directive

The Alberta Government has an overall responsibility to ensure that the provision of services for, and on behalf of, all Albertans are undertaken in an open and accountable manner. The increased delegation of responsibilities to managers in order to facilitate the necessary streamlining and efficiencies in decision-making, along with the increased expectations of the public for accountability are factors that have led the Public Service Commissioner after consultation with the Deputy Minister's Committee, to review the need for strengthened security screening processes. The intent of the Directive is to ensure a sufficient degree of due diligence in the hiring or reclassifying of designated positions, who by virtue of their heightened degree of responsibility, and public trust, should withstand this level of scrutiny.

The decision has been made, in consultation with the Deputy Minister's Committee, by the Public Service Commissioner to issue the Directive as a means of screening new appointments. In addition, the Deputy Minister's Committee recommended that the process also be applied on a voluntary basis, to existing staff who meet the criteria for the Enhanced Security Screening level within the Alberta Security Screening Directive according to their current positions.

1.5 Current Situation

Currently the main type of security screening required as part of the public service recruitment or reclassification process is a Criminal Records Check, as determined by each Ministry. In addition, Alberta Economic Development currently uses a process conducted by the Canadian Security Intelligence Service (CSIS) to screen candidates for foreign postings.

Individual Ministries identify those positions that require Criminal Records Checks based on one or more of the following criteria:

- Positions of trust where the client relies on the character or truth of the employee. **Note:** While all employees can be said to occupy a "position of trust", this criteria is interpreted as focusing on those positions that have significant client contact and/or where the well being of the client is in some way based on decisions made by the employee, such as Human Service or Group Home Workers.
- Positions charged with special status or designation.
- Positions dealing with court proceedings and evidence admitted to the court.
- Positions in contact with highly confidential/sensitive information or large amounts of cash, goods or restricted drugs.

The Criminal Records Check is coordinated through the Human Resources Advisor responsible for managing the appointment of an employee through competition or through an exemption. The most common process is for the individual to have the local police provide them with a certificate. The individual then submits the certificate to the Human Resources Advisor. In one Ministry, a process has been established to have prospective appointees sign a consent form authorizing the employer to obtain a criminal records check on their behalf.

1.5.1 Limitations of Current Security Screening Processes

The current security screening process is not sufficient to meet the intent that has been identified for the proposed Directive.

1.5.2 Implications of the Directive on Current Security Screening Processes

The implementation of the Directive is not intended to significantly change the current process for conducting a Criminal Records Check for Ministry-identified positions. Ministries will continue to have the flexibility to identify positions which they feel meet the criteria identified above and to require a Criminal Records Check be conducted prior to an appointment or reclassification being made to that position. Ministry identified positions will come under the Directive.

Ministries will **not** have the authority to add specific positions to those listed in the Directive for the Enhanced Security Screening without consultation with the Deputy Minister of Executive Council.

1.6 Scope of the Alberta Security Screening Directive

The Directive introduces an additional level of security screening beyond that of a Criminal Records Check and identifies the specific positions that each level applies to (see Appendix 1). The positions identified at each level are representative of increasing responsibility, thereby requiring more thorough screening.

All positions that require security screening have been determined to meet some or all of the following criteria:

- Positions of trust where the client relies on the character or truth of the employee
- Positions charged with special status or designation
- Positions dealing with court proceedings and evidence admitted to the court
- Positions in contact with highly confidential/sensitive information or large amounts of cash, goods or restricted drugs.

The security screening results for all positions noted in this Directive are reviewed and assessed for any required follow-up action by designated official(s) listed in the Directive.

The type of security screening required will be dependent on the classification hierarchy (see Appendices 1 and 2). There are two security levels and three screening components:

- Level 1 – Criminal Records Check – Criminal Records Check only
- Level 2 – Enhanced Security Screening -- Criminal Records Check *plus* Financial Management Risk Indicator Screening *plus* Vulnerability Risk Indicator Screening

The screening components are described in sections 1.6.1 to 1.6.3 below.

Security screenings will be required for all future appointments or reclassifications to the positions identified in the Directive.

Current employees in the positions identified as requiring an enhanced security screening have the option of volunteering to participate in the screening process.

Consent of the individual will be required before a security screening can be initiated.

The implementation of the Directive will result in a common, consistent process to be used by the employer on behalf of the Government of Alberta (as described in Appendix 2).

1.6.1 Criminal Records Check (Level 1 & 2)

A Criminal Records Check involves a screening for the presence of criminal convictions, against the Canadian Police Information Center (CPIC). The screening is conducted by the applicable local police force.

While the intent of the Directive is to incorporate as much as possible, the Criminal Records Check procedures that Ministries currently use, the procedures will be subject to the rules established by the Directive.

In all cases where a Criminal Records Check is required, individuals will be given the option to provide a certificate from the applicable police force themselves. Where the individual chooses to have the Ministry collect the Criminal Records Check information, the certificate will be made accessible to the individual upon request.

1.6.2 Financial Management Risk Indicator Check (Level 2 only)

A Financial Management Risk Indicator Screening involves a screening for the presence of financial management risk indicators such as bankruptcies, garnishees, credit payments beyond 90 days, poor credit rating and the like. The information that will be requested will be limited to the general information as outlined in Appendix 5.

Details of the individual's financial and credit information are **not** disclosed in the report to the employer.

The purpose of this screening is to identify the potential for risks to the employer where an individual has fiscal responsibility for budgets, expenditures or by their participation on Executive Committees through which they have input to, and influence on, program decisions taken by the Ministry.

The individual will be provided every opportunity to discuss any perceptions of risk that are raised as a result of the information that is received by the employer.

TransUnion is the credit bureau that has been contracted with to act as the Government of Alberta's agent for conducting Financial Management Risk Indicator Screenings. In all cases where a Financial Management Risk Indicator Screening is required, individuals will be given the option to provide a certificate from TransUnion themselves. Where the individual chooses to have the Ministry

collect the Financial Management Risk Indicator Screening information, the certificate will be made accessible to the individual upon request.

1.6.3 Vulnerability Risk Indicator Screening (Level 2 only)

The Canadian Security Intelligence Service (CSIS) is being contracted with, to act as the Government of Alberta's agent for conducting Vulnerability Risk Indicator Screenings. CSIS screens applicant's information against the CSIS data bases for the following issues:

- Espionage or sabotage
- Foreign influenced activities
- Threat or use of serious violence to achieve a political, religious or ideological objective
- Political violence leading to the destruction of the established system of the government of Canada.

CSIS will conduct the screening only with the signed consent of the individual. CSIS may interview the individual about any information where there may be some clarification required regarding an issue, in order to provide the individual with an opportunity to clarify or elaborate on the information that has been collected.

The individual will only have access to information gathered about them through application directly to CSIS, with the exception of information that is protected under Federal Legislation.

CSIS will only match the information requests from the Provincial Government against their existing databases. The information that is provided to the Provincial Government as a result of that search will not create a new database, nor set up a new file to be maintained by CSIS. A match that results in disclosure will be documented on the associated disclosure log, as is required under the Federal legislation (*Privacy Act*, section 9).

1.7 Benefits

Benefits derived from this Directive will include the ability to assure Albertans that the employer, on behalf of the Provincial Government, has been duly diligent in recruiting, appointing or reclassifying individuals to designated positions who will have a responsibility for the stewardship of government resources and meet one or more of the criteria outlined in section 1.6. At the same time, the Directive provides a balance between those individuals' rights to privacy while they undergo a security screening, and maintaining accountability to Albertans. The

employer will be able to ensure that any concerns raised through either level of security screening have been reviewed and assessed at the time of hire, appointment or reclassification.

1.8 Timing

The employer will choose an effective date for the implementation of the Directive for future designated employees, once this assessment is accepted by the Information and Privacy Commissioner. The process will also be extended to those current employees in positions designated in the Directive, as requiring an Enhanced Security Screening who volunteer to undergo an enhanced security screening.

2.0 PERSONAL INFORMATION COLLECTED, USED AND DISCLOSED

2.1 Personal Information Collected

Consent of the individual is required before the security screenings can be initiated. Individuals who choose not to provide their consent will not have their application for employment considered further.

The type of screening required will be dependent on the position as designated in the Directive. There are two security levels and three screening components (see *Figure 1*).

The information that individuals must provide to initiate the screening process is shown in Appendix 3.

Appendix 5 shows the personal information that will be reported as a result of the Financial Management Risk Indicator Screening.

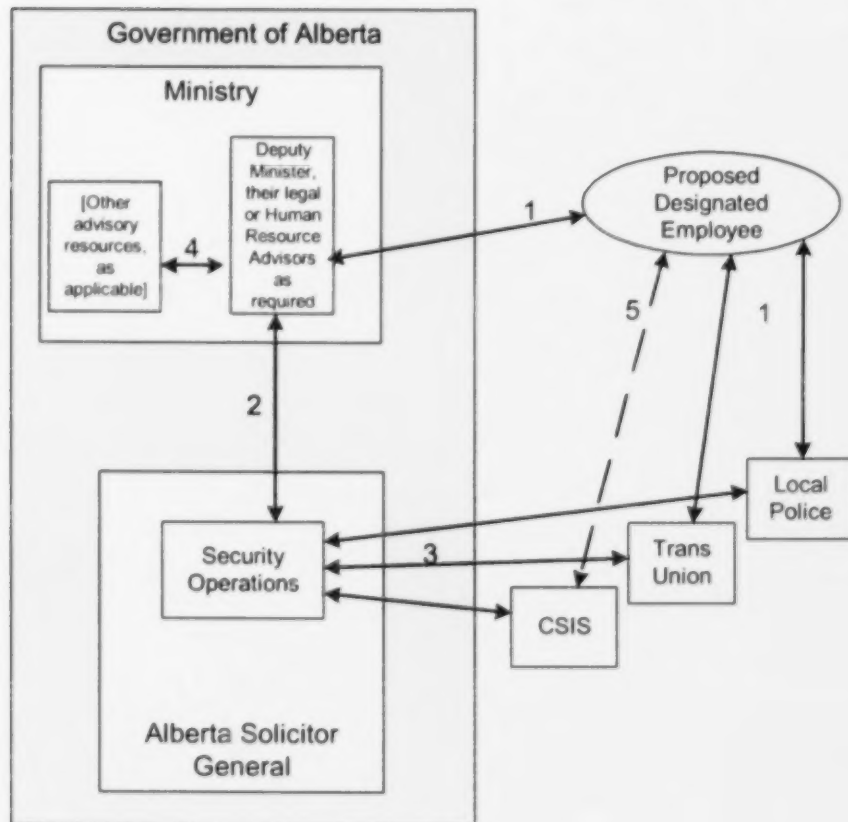
Figure 1
Personal Information Collected

Level 1 – Criminal Records Check		
Type of Check	Personal Information Provided by the Individual	Report Containing Personal Information Provided by:
Criminal Records Check	See <u>Appendix 4</u>	Local Police Service
Level 2 – Enhanced Security Screening		
Type of Check	Personal Information Provided by the Individual	Report Containing Personal Information Provided by:
Criminal Records Check	See <u>Appendix 4</u>	Local Police Service
Financial Management Risk Indicator Screening	See <u>Appendix 5</u>	TransUnion
Vulnerability Risk Indicator Screening	See <u>Appendix 6</u>	Canadian Security Intelligence Service

2.2 Information Flows

Appendix 2 describes the security screening process. The information flows resulting from these processes are shown in *Figures 2 and 3*. A description of the information flows follows each figure.

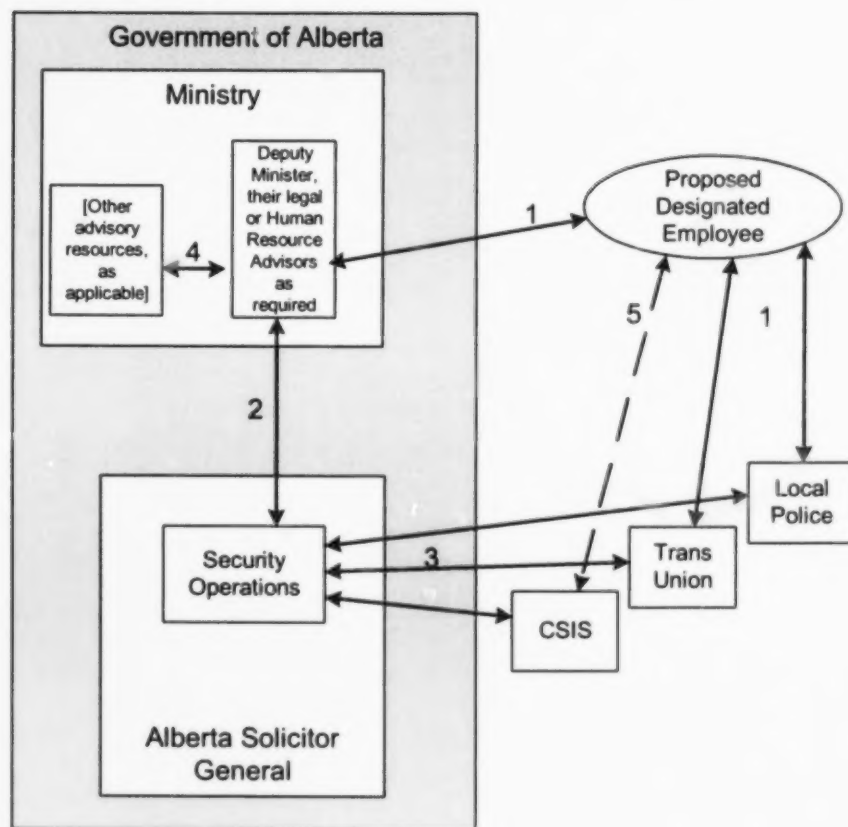
Figure 2
Security Screenings Information Flow
Future Employees (as per Directive – Appendix 1)



2.2 Information Flows

Appendix 2 describes the security screening process. The information flows resulting from these processes are shown in *Figures 2 and 3*. A description of the information flows follows each figure.

Figure 2
Security Screenings Information Flow
Future Employees (as per Directive – Appendix 1)



Security Screenings Information Flow - Future Employees (Description)

1. The individual provides consent to the Deputy Minister or designate to carry out the applicable security screening (Level 1 or Level 2) or alternatively, the individual can obtain the security screenings directly from the local police service and TransUnion. A Level 1 security screening involves only a Criminal Records Check. The CSIS screening for a Level 2 security screening must be done through Security Operations as coordinated by the Ministry or Executive Search within PAO.

Where the individual has chosen to obtain the security screenings directly, the contracted agents forward the report directly to the individual. The individual then forwards the report(s) to the Human Resources Advisor.

If the individual wishes to request a correction, they must make a request to the source of the report.

Where the Ministry or Executive Search has initiated the security screening process with the written consent of the individual, copies of the Criminal Records and Financial Management Risk Indicator Screening reports will be released to the individual as a matter of routine disclosure.

2. The Human Resources Advisor forwards the appropriate consent forms to Security Operations.

Security Operations forwards reports to the Human Resources Advisor (see 3 below).

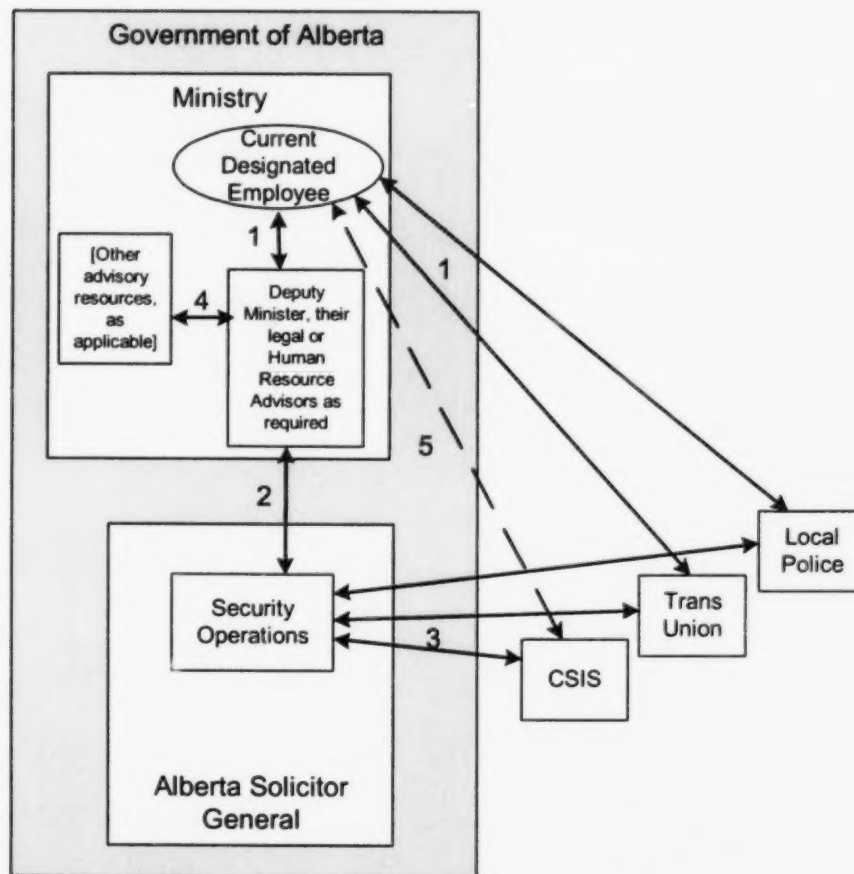
3. Security Operations forwards the appropriate forms to police and TransUnion. Security Operations will enter the personal information contained on the forms directly into the secure electronic system (provided by CSIS).

These contracted agents return completed reports to Security Operations. All forms submitted to Security Operations will be retained in their custody on behalf of the employing department.

4. The Deputy Minister may consult with advisors regarding the report.
5. CSIS may interview the individual for clarification of potential issues.

If the individual wishes to access the report or to request a correction, they must make a request to CSIS.

Figure 3
Security Screenings Information Flow
Current Employees (as per Directive – Appendix 1)



Security Screenings Information Flow - Current Employees (Description)

1. The individual provides consent to the Deputy Minister, or designate, to carry out the applicable security screening (Level 2) or alternatively, the individual can obtain the security screenings directly from the local police service and TransUnion. The CSIS screening for a Level 2 security screening must be done through Security Operations as coordinated by the Ministry.

Where the individual has chosen to obtain the security screenings directly, the contracted agents forward the report directly to the individual. The individual then forwards the report(s) to the Human Resources Advisor.

If the individual wishes to request a correction, they must make a request to the source of the report.

Where the Ministry has initiated the security screening process with the written consent of the individual, copies of the Criminal Records Checks and Financial Management Risk Indicator Screening reports will be released to the individual as a matter of routine disclosure.

2. The Human Resources Advisor forwards the appropriate consent forms to Security Operations.

Security Operations forwards reports to the Human Resources Advisor (see 3 below).

3. Security Operations forwards the appropriate forms to police and TransUnion. Security Operations will enter the personal information contained on the forms directly into the secure electronic system (provided by CSIS).

These contracted agents return completed reports to Security Operations. All forms submitted to Security Operations will be retained in their custody on behalf of the employing department.

4. The Deputy Minister may consult with advisors regarding the report.
5. CSIS may interview the individual for clarification of potential issues.

If the individual wishes to access the report or to request a correction, they must make a request to CSIS.

2.3 Information Users

2.3.1 The Individual's Ministry

For prospective employees, screenings would be conducted before an offer of employment is extended. In some situations, the completion of a screening may be required at the time of being short-listed as one of several potential top candidates, or in order to receive certification of being eligible for any future vacant positions. For current employees, participation in the security screening process is voluntary. No screening will occur before the individual's written consent is obtained.

The Human Resources Advisor for that Ministry is responsible to ensure that consenting individuals have completed and submitted a Criminal Records Check or Financial Management Risk Indicator Screening as applicable, to their office, or signed a consent form and appropriate application forms to allow the Ministry to collect the information from the contracted agents.

Normally the management representative to whom the position reports will be the Ministry representative evaluating information obtained through the security screenings. The Human Resource Advisor may also be called upon to assist management in assessing the relevance of a security screening to the position duties. *Appendix 1* identifies the users in the individual's Ministry to whom a screening can be disclosed.

2.3.2 Role of Executive Search, PAO

Executive Search within the PAO, is responsible for the recruitment of senior level management positions on behalf of the Ministries in the Government of Alberta. In this role, Executive Search becomes the Human Resources Advisor recruiting to senior level positions and is responsible for managing the recruitment process in accordance with the *Public Service Act*, on behalf of the Ministry that the position will report to. Executive Search will ensure that the proper level of security screening is received prior to an appointment being made.

2.3.3 Role of Security Operations, Alberta Solicitor General

Under the security screening processes described in *Appendix 2*, the human resources advisor, **only with the prior consent of the individual**, requests Security Operations to coordinate a security screening. Security Operations transmits personal information to the appropriate agency to conduct the actual screening. Information about the individual is collected from the applicable third party sources identified in sections 1.6.1 to 1.6.3 in Chapter 1.

Security Operations does not evaluate information about any individual that is submitted to it by the contracted agencies.

Section 40(1)(i) of the *Freedom of Information and Protection of Privacy Act* allows public bodies to disclose personal information to an official of another public body where they are involved in the delivery of a common program or integrated service. As stated at the outset of the PIA, the Government of Alberta as one employer is impacted by the Directive in the delivery of an integrated human resource service and program.

2.3.4 Role of the PAO

Except as noted in section 2.3.2 above, the PAO does not have any direct involvement in the collection, use and disclosure of personal information collected as a result of a security screening. The staff within the PAO may be called upon by Ministries to provide functional expertise in areas related to the Directive.

PAO has the responsibility under the *Public Service Act* for the development and implementation of the Alberta Security Screening Directive. Through training and communication initiatives, PAO ensures that the Ministries have an understanding of the Directive and are aware of the screening process and supporting activities.

3.0 PROTECTION OF PERSONAL INFORMATION ANALYSIS

3.1 Collection of Personal Information

Section 33 of the *FOIP Act* requires that public bodies have authority to collect personal information. Most often, legislation will give authority for a particular program or activity without authorizing the collection of specific personal information. In these situations, and in this case, section 33(c) of the *Act* applies to the Alberta Security Screening Directive.

33 *No personal information may be collected by or for a public body unless*

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

The Personnel Administration Office (PAO), will not be collecting personal information. Sections 3.1.1 to 3.1.3 as follows, describe the PAO's authority to establish government-wide direction in personnel matters (e.g. through the use of policies, directives and regulations). Public bodies that are subject to the *Public Service Act* are required to adhere to corporate directions established by PAO and recognizing that the Government of Alberta is one employer.

Section 3.1.4 describes the affected public bodies' authority to manage personnel activities. The discussion in these sections establishes the setting and implementation of personnel policies as a legitimate operating program or activity.

Section 3.1.5 describes the legislative authority to collect personal information in support of the Directive.

3.1.1 Authority of PSC to Set Personnel Policy

The *Public Service Act* [s.6(1)] provides the Public Service Commissioner with the general authority to:

- provide advice on personnel policy, legislation and administration to the Minister Responsible for the Personnel Administration Office (PAO) and to the Government of Alberta;
- develop and administer systems to carry out human resource policies and practices;
- manage a comprehensive personnel program for the Alberta Public Service;

- provide advice and assistance to senior department managers on personnel matters; and
- support the Government Reorganization Secretariat.

This general authority establishes the Public Service Commissioner's mandate to develop, apply, and review the appropriate personnel activities for the Alberta Government as one employer, including setting and maintaining personnel policy and ensuring that policy is applied in a consistent manner across all Ministries.

In the case of the Alberta Security Screening Directive, in consultation with the Deputy Minister's Committee, the Public Service Commissioner determined that a Criminal Records Check, a Financial Management Risk Indicator Screening and a Vulnerability Risk Indicator Screening is required for all new appointments or reclassifications to the positions/classifications identified in the Directive, dependent on the level and function of the position in question.

3.1.2 Application of Directive for New Hires and Appointments

When a position is to be filled by in-service promotion or by limited or open competition, or is exempt from competition, an appointment to the position is subject to certification that the person to be appointed is qualified for the position. A security screening for those positions identified above will be completed as part of that process.

The *Public Service Act* gives the Public Service Commissioner explicit authority to determine appropriate hiring criteria. Sections 17(3) and 18(3) enable the Public Service Commissioner to put in place rules and procedures for competitions and subsequent appointment to a position.

17(3) Competitions conducted by a department head must be conducted in accordance with the rules and procedures prescribed by the Commissioner.

18(1) All appointments to positions in a classification plan shall be made by the department head.

(2) When a position

(a) is to be filled by in-service promotion or by limited or open competition, or

(b) is exempt from competition under section 16(3)(a) or (b),

an appointment to the position is subject to certification that the person to be appointed is qualified for the position.

(3) The certification shall be made in accordance with the directions of the Commissioner and by the persons authorized to do so by those directions.

(4) Appointments made to positions excluded from a classification plan pursuant to section 11 shall be made by order of the Lieutenant Governor in Council on the recommendation of the department head.

3.1.3 Application of Directive to Current Employees

The Directive will be applied to existing staff who meet the criteria for an enhanced security screening in the Directive according to their current positions, but on a voluntary basis.

The Public Service Act enables the Public Service Commissioner to set personnel policy and apply it to current employees. Sections [6(1)(a) and (c), 2 and 10] of the Public Service Act provide implicit support of the Commissioner's authority to set personnel policy and apply it to current employees.

It is important to assure Albertans that the Government of Alberta, as one employer, has made every reasonable effort to ensure that due diligence has occurred with respect to the individuals who are currently stewarding resources.

The Public Service Act [s.6(1)] provides the Public Service Commissioner the general authority to:

- (a) advise the Minister respecting personnel policies, regulations and procedures;*
- (d) advise and assist departments in the conduct of departmental personnel activities [emphasis added];*

Section 2 of the Public Service Act establishes the scope of that Act, and identifies that individuals who are employed, subject to the Act, are deemed employees of the Crown:

- 2(1) Except as otherwise provided in this Act or any other enactment, this Act applies to all departments.*
- (5) A person who is appointed or employed*
 - (a) in accordance with,*
 - (b) pursuant to, or*
 - (c) subject to,**this Act, is an employee of the Crown in right of Alberta.*

Section 10 of the Public Service Act goes on to establish the authority to create classification plans for those employees, in order to ensure that there is a consistent or uniform process to administer those employees.

- 10(1) The Minister may with the approval of the Lieutenant Governor in Council establish one or more classification plans defining and designating the classes of positions in the public service*

- (a) as a basis for uniform treatment of employees performing the same kind and level of work, and
- (b) to provide a systematic basis for organization and administration.
- (2) Each position in a department shall be allocated to a class in a classification plan by the Commissioner.
- (3) The Minister may from time to time amend a classification plan without the approval of the Lieutenant Governor in Council.

As such, the Public Service Act clearly identifies that there should be a process that applies to all employees, whether hired or appointed, and that the process applies to employees across all government departments.

3.1.4 Authority of Deputy Ministers to Manage Personnel Activities

While, as noted in the previous section, the Public Service Commissioner has the authority to set personnel policy, the activities required to support these policies are the responsibility of the Ministries. Ministerial authority is derived from the Public Service Act and the Government Organization Act.

Section 8 of the Public Service Act establishes the responsibilities of the Deputy Head (Deputy Minister) relating to personnel matters.

- 8(1)** Subject to the general direction of the department head, the deputy head
- (a) shall oversee and control the attendance, conduct and work performance of the employees in the deputy head's department,
 - (b) may, subject to any other Act relating to the organization of a department, divide the department into branches and divisions and assign duties to positions as required for the effective performance of the department's functions, and
 - (c) may appoint an acting officer to have, during the absence of the incumbent, the power and authority of the office for which the acting officer is appointed to act, unless such an appointment is otherwise provided for by any other Act.
- (2) For the purposes of this Act, a deputy head has the powers and may perform the duties of the deputy head's department head.
- (3) A department head may appoint an employee of that department as the acting deputy head of that department, and an acting deputy head so appointed has, during the absence of the deputy head or a vacancy in the office of the deputy head, the powers and duties of the deputy head.

In addition, the Government Organization Act allows for a Minister to establish or operate any program considered desirable:

8(1) A Minister may establish or operate any programs and services the Minister considers desirable in order to carry out matters under the Minister's administration.

(2) A Minister may institute inquiries into and collect information and statistics relating to any matter under the Minister's administration.

Such programs and services could and do include the personnel programs and activities necessary to effectively operate the Ministry and fulfill the responsibilities that are required under Section 8 of the Public Service Act.

3.1.5 Authority to Collect Personal Information

The *Public Service Act* and the *Government Organization Act* as described above in sections 3.1.1 to 3.1.4 above, authorize the Personnel Administration Office and the individual Ministries to carry out human resource management activities.

Authority to collect personal information is derived from section 33(c) of the *Freedom of Information and Protection of Privacy (FOIP) Act*:

33 No personal information may be collected by or for a public body unless

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

Under the Alberta Security Screening Directive, personal information is collected from the prospective or current employee to support a Criminal Records Check, a Financial Management Risk Indicator Screening and a Vulnerability Risk Indicator Screening. As with other screenings, such as reference checks or education verification checks, the results may not necessarily ensure that an individual is able to attend to his/her responsibilities in an appropriate manner, but the screenings serve as a discussion point with the individual should there be any issues identified through the various screening processes. As is the case in all recruitment or reclassification activities, reasonable and diligent judgment should be used in assessing all of the information known about a candidate in making the final decision. The Security Screening Directive adds additional information that must be analyzed and weighed.

As described in section 2.1, *Collection of Personal Information*, the personal information to initiate a screening is supplied by the individual while third parties prepare the reports containing personal information. In support of these two activities, the employer determined:

- the exact personal information which is needed to carry out the screening and no more; and,

- that the content of the screening reports provided to the employer is summary information and limited to that information that provides an indicator.

These reports are prepared by third parties who have established screening processes. As such, the directive identifies classes or position designations that are to undergo the screening.

Use of the personal information obtained from the collection is discussed in section 3.6.

3.2 Manner of Collection of Personal Information

Section 34(1) of the *FOIP Act* establishes direct collection as the primary method for obtaining personal information. The same section also authorizes indirect collection of personal information with the informed consent of the individual.

*34(1) A public body must collect personal information directly from the individual the information is about unless
(a) another method of collection is authorized by
i. that individual*

The intent of section 34 is to ensure that an individual is aware of the type of personal information being used to make a decision concerning him or her.

The Directive will be applied to existing staff on a voluntary basis who meet the criteria for an enhanced security screening in the Directive according to their current positions.

The personal information provided by the third party agents is an indirect collection of information and is thus subject to s.34(1)(a)(i) of the *FOIP Act*. Criminal Records Checks (completed by local police departments) will only be completed if the individual to whom the check pertains has completed and signed a consent and authorization. (See Appendix 4). Likewise, screenings that are completed by TransUnion or the Canadian Security Intelligence Service (CSIS) will only be completed if the individual to whom the screening pertains has completed and signed an authorization (see Appendix 5 and Appendix 6).

In the case of Criminal Records Checks and Financial Management Risk Indicator Screenings, the individual has the option of obtaining the reports directly and submitting them to his/her Ministry's Human Resources Advisor (Level 1) or Deputy Minister (Level 2). See sections 1.6.1 and 1.6.2 for more information. Under the *FOIP Act*, this is a direct collection of personal information in accordance with s. 34(1).

In those instances where the individuals choose to sign a consent authorizing the employing Ministry to obtain Criminal Records Checks and Financial Management Risk Indicator Screenings on their behalf, this is an indirect collection under 34(1)(a)(i) of the *FOIP Act*. As well, CSIS does not conduct security screenings on behalf of individuals and hence the request must be handled through Security Operations on behalf of the Ministry. Individuals must sign a consent authorizing the employing Ministry to obtain Vulnerability Risk Indicator Screening from CSIS. See Appendix 3 for the applicable consent forms for this indirect collection.

The forms filled out by the consenting applicant for the Criminal Records Check and Financial Management Risk Indicator Screening collect information only on the applicant. The Vulnerability Risk Indicator Screening form also requests information about the applicant's current or former spouse/common-law partner. This third party information is collected to ensure a complete database search of potential links to the applicant. There is no screening done on the third party. The collection of information about the applicant's current or former spouse/common-law partner in these circumstances is authorized by section 34(1)(n) of the *FOIP Act*.

3.3 Accuracy and Retention

3.3.1 Accuracy

The Criminal Records Checks, Financial Management Risk Indicator and Vulnerability Risk Indicator Screenings required by the Directive are carried out by contracted third parties: local police services, TransUnion and CSIS, respectively.

These agents are responsible for the accuracy of the reports they provide – the information that is used to complete the reports is based on information maintained by that organization, or on the basis of information that is submitted to the organization by the individual. If the individual questions the accuracy of the information obtained, they should address their concerns to the applicable contracted agent. The individual will also be given the opportunity to present further information to the Ministry (see 3.4 Right to Request Correction).

CSIS has identified that they would require a single point of contact with the Alberta Government, as managing the requests from 23 ministries would not be practical. As a result, Security Operations within Alberta Solicitor General was identified to be that contact. Security Operations was chosen due to their knowledge of security matters in general, the fact that all staff currently have a security screening with CSIS, and they are currently the agent of the Alberta Government who coordinates with CSIS on other security matters.

As noted in the previous section, individuals have the option of obtaining Criminal Records and Financial Management Risk Indicator Screenings (as applicable) directly from the contracted agents.

In those cases where the individual has authorized the Ministry to obtain the screening, information that is received from the local police service and TransUnion will be routinely presented to the individual upon request. Disclosures from CSIS to Security Operations are on the basis that the information will not be provided to the individual. A request for this information under the *FOIP Act* would be denied under s. 21(1)(b) and s. 21(3). The former allows the head of a public body to refuse to disclose information on the basis that the disclosure could reveal information supplied in confidence by CSIS which is an agency of the Government of Canada. The latter provides that a public body may disclose information supplied in confidence only with the consent of the agency that supplied the information. The individual can request this information from CSIS. Formal requests for this information are subject to the *Privacy Act*, which is Federal legislation.

Individuals will be provided the opportunity to address any issues that may be seen in the Criminal Records Check if they are deemed to be relevant to the decision in the appointment or reclassification to the position. Information that is received from TransUnion will be limited to Financial Management Risk Indicators, and not the actual detailed credit history. Individuals will be provided the opportunity to address any issues identified in the Financial Management Risk Indicators. CSIS will interview the individuals as a part of their process should they identify any potential issue requiring clarification regarding the security screening.

3.3.2 Records Retention

Security Operations will maintain the original copies, on behalf of the Ministries, of the following information collected as a result of the security screening process:

- Information that is submitted by the individual, which is included on the forms that they complete (see *Appendix 4*)
- Responses submitted by the individual to the Ministry
- Responses obtained from police agencies to the Criminal Records Check. [Note: Criminal Records Checks completed by the individual Ministries are maintained on the individual competition file.]
- Responses obtained from TransUnion to the Financial Management Risk Indicator Screening. (See *Appendix 5*)
- Information provided by CSIS for the Vulnerability Risk Indicator Screening.
- Responses to the Security Screening request sent by CSIS.

The records maintained by Security Operations will be retained in accordance with the *Administrative Records Disposition Authority*.

Ministries will receive copies of reports from Security Operations. These are treated as transitory documents, which are destroyed once they have served their purpose.

A checklist form (Appendix 3) will indicate whether the screening was completed. This form will be retained by the Ministry in the individual's personnel file or competition file as applicable. This form is retained in accordance with the retention and disposition schedules under the *Administrative Records Disposition Authority*.

3.4 Right to Request Correction of Personal Information

As described in the previous section, requests for corrections must be made to the source of the report. While the Ministry has no authority to correct information collected and reported by a contracted agent, it will afford the individual the opportunity to provide further information or documentation that may result in a correction or annotation to the records. This will be clearly identified to the individual should the need arise.

Note that security screenings conducted by CSIS will be subject to correction under the Federal legislation [*Privacy Act*, s.12(2)]. As a matter of course, if an issue arises during the processing of the screening, CSIS will interview the individual and provide them with the opportunity for clarification.

3.5 Protection of Personal Information

Information obtained by Security Operations from the contracted agents is retained in a secure environment at Solicitor General.

If the information reviewed by CSIS does not result in a match against the database maintained by CSIS, that will be reported in writing directly to Security Operations, via secure electronic mail as a "No Reportable Trace". If there are concerns identified through a match in the CSIS database, that information will also be provided in writing via secure electronic mail, directly to Security Operations.

Security Operations advises the employer of the outcome. Access to original CSIS reports is tightly restricted, and will be managed by Security Operations, as identified in section 3.5.1 below. The information maintained in the reports is accessible (generally in a summary format) by the applicable Ministry's Deputy

Minister or the Deputy Minister of Executive Council in accordance with the chart in the Alberta Security Screening Directive (Appendix 1).

The process by which the personal information is transmitted is identified in section 3.5.1 below.

While Security Operations retains custody of the original information on behalf of the employer, the Ministry to whom the individual reports, is responsible for the control of that personal information. Security Operations keeps the original information in a secure facility. Filing cabinets will be locked, as will the offices they are contained in. In addition the office area is monitored 24 hours per day by video surveillance.

The rationale for the maintenance of the information by Security Operations is to ensure strict protection of the personal privacy of the individuals who have completed to an enhanced security screening. Individuals to whom the information pertains will have a right of access to that information, subject to the applicable legislation (e.g. information held by CSIS needs to be accessed through federal legislation).

3.5.1 Security Provisions for Transmittal and Storage of Personal Information

Storage:

Personal information that is used and stored by CSIS staff is handled in a secure manner, according to strict security provisions. Staff having access to the information will be limited to those conducting the matching and assessment of the information against CSIS' database. The CSIS database comprises information on individuals that have come to the attention of CSIS through a mandated investigative process. In the event that there is insufficient data to determine whether or not an exact match occurs, a further analysis may be undertaken that may include contact with the individual.

Where matches against the CSIS database occurs, that information is summarized and provided in a summary format to Security Operations.

Transmittal:

Information that is submitted by the (potential) employee on the forms will be used to complete an electronic template that is provided by CSIS. The data will be sent to CSIS HQ in Ottawa, via a secure electronic process. The e-mail and any attachments will be encrypted, and sent through a Public Key Infrastructure (PKI) process. CSIS will provide an authentication certificate (PKI) to designated staff in the Security Operations Branch.

Similarly, any information that is sent in an electronic manner to Security Operations will be sent in an encrypted form, and using PKI technology and authentication processes.

Note that no additional databases outside of those maintained by CSIS are researched by CSIS staff as they assess and complete the clearance.

3.6 Use of Personal Information

Personal information that is collected and reviewed through the implementation of this Directive is only to be used for the purposes described in sections 1.6.1 – 1.6.3 and Appendix 1.

The existence of a positive or negative security screening will not automatically result in the offer or denial of a position or have any impact, positive or negative, on an existing employee. The relationship between the result of the screening and the duties of the position that the individual is applying for is being reclassified to, or holds, will be reviewed on an individual basis. A determination of the consequences of any decision regarding that relationship will be made by the Employer in consultation with legal and/or human resource advisors.

It should be noted however, that the manner in which this process will unfold is a Human Resources matter, and is outside the scope of this PIA.

3.7 Disclosure of Personal Information

Information is disclosed only to the authorized users (see Appendix 1). The information flow diagrams in *Figures 2 and 3* will assist in identifying that disclosure. Note that the flow diagrams refer to the individuals identified in the Alberta Screening Directive (as per Appendix 1).

The Security Operations Branch of Alberta Solicitor General acts on behalf of the employer and has been authorized by the employer to collect information with an individual's consent and to disclose information only to either the employer or to the individual the information has been collected about and has no authority to use or disclose information on its own. As such, Security Operations:

- Is responsible for collecting, maintaining and securing the personal information from the local police and TransUnion (where the individual has consented in writing) and all requests for screenings from CSIS (see section 3.2).
- Discloses to the employer the results of the requested security screenings.

- Maintains custody and protects the information on behalf of the employer.
- Manages the contracts with the third parties who conduct the screenings.

Other than to the individuals to whom the information from the screening relates, there will be no routine disclosures of personal information collected as a result of the Directive. Any request for disclosure of this information must be with the individual's consent or in accordance with section 40 of the FOIP Act [e.g. s.40(1)(h) – disclosure for the management or administration of personnel who need it to do their business].

3.8 Disclosure for Research or Statistical Purposes

It is not anticipated that personal information would be disclosed for research or statistical purposes. However, given that there is discretion within the *FOIP Act* to disclose information for research and statistical purposes, any request for information will have to be reviewed by the employer through a Ministry in consultation with PAO.

4.0 POTENTIAL PRIVACY IMPACTS

4.1 Potential Privacy Impacts

Individuals who are applying for or seeking appointment or reclassification to positions that are designated by the Directive will be advised in advance of the requirement for a security screening. This applies to current Government of Alberta employees who are applying for a new position.

Should the security screening identify issues of concern to the employer, individuals will be given an opportunity to provide additional clarifying information. Individuals will be able to contact the credit agency to obtain a detailed report of their financial information. The employer will disclose information it has obtained from a police agency. CSIS information will be disclosed subject to federal legislation.

Security Operations will maintain personal information that is obtained through the security screening. Ministry Human Resources staff will be limited to access only the information that relates to the individuals seeking employment, or employed, by that Ministry.

Staff currently occupying a position that is designated by the Directive as subject to a security screening may voluntarily complete a security screening.

Individuals must authorize the collection and disclosure of the screening information. (See Release of Information Consent Form – Appendix 3) Should they choose not to consent, in the case of recruitment, no employment offer would be extended.

4.1.2 Conclusion

The expectations that citizens have of the need for security and privacy extends not only to the information that government organizations maintain about them, but also to the integrity of the individuals who are hired, appointed, or reclassified to positions of trust within those organizations. The Personnel Administration Office, in consultation with the Deputy Ministers, advances that those positions designated in the Security Screening Directive are in positions of trust within the public service. There is a need to properly apply a screening process to deal with issues that have the potential to impact on the areas of responsibility of the individuals in those positions of trust.

5.0 APPENDIX 1**5.1 Alberta Security Screening Directive**

Security screening is required for all appointments or reclassifications to the positions/classifications identified below:

Type of Security Screening: Level 1 –Criminal Records Check		
APPLIES TO:	COLLECTED BY:	INFORMATION DISCLOSED TO:
Senior Officials appointed by Order in Council.	Security Operations on behalf of the Ministry.	Deputy Minister of Executive Council or the appropriate Board or Commission Chair, and their legal or human resource advisors as required.
All Management positions in the Alberta Public Service. All Accounting Officers. All Expenditure Officers. Positions as determined by the Deputy Minister.	Ministry Human Resource Director or Executive Search.	Appropriate Deputy Minister, or Management Representative and/or their legal or human resource advisors as required.
Type of Security Screening: Level 2 – Enhanced Security Screening		
APPLIES TO:	COLLECTED BY:	INFORMATION DISCLOSED TO:
Members DM Committee. Members of Ministry Executive Committees. Senior Financial Officers. Positions as determined by the Deputy Minister in consultation with DM, Executive Council.	Criminal Records Check and Financial Management Risk Indicator Screening are collected by Security Operations on behalf of the employer. Vulnerability Risk Indicator Screening through Canadian Security Intelligence Service (CSIS.), are collected by Security Operations on behalf of the employer.	Deputy Minister Executive Council or appropriate Deputy Minister, their legal or human resource advisors as required.

All positions that require security screening are determined to meet some or all of the following criteria:

- Positions of trust where the client relies on the character or truth of the employee
- Positions charged with special status or designation
- Positions dealing with court proceedings and evidence admitted to the court
- Positions in contact with highly confidential/sensitive information or large amounts of cash, goods or restricted drugs.

The security screening results for all positions noted in this directive are reviewed and assessed for any required follow up action by the official(s) listed as having access to the information. In all cases where a Criminal Records Check or Financial Management Risk Indicator Screening is required, the applicants will be given the alternative to provide a certificate from the applicable police force or credit bureau themselves. Criminal Records Check information collected through Security Operations will be made accessible to the applicant upon request.

Ministries will file a list of the positions determined by the Deputy Minister, that require security screening with the Public Service Commissioner's Office by March 31 of each year.

DEFINITIONS

For the purposes of this Directive the following definitions apply:

Criminal Records Check: involves a screening, for the presence of criminal convictions, against the Canadian Police Information Center (CPIC), based on name and birth date and is conducted by the applicable police force.

Financial Management Risk Indicator Screening: involves a screening for the presence of Financial Management Risk Indicators such as bankruptcies, garnishees, credit payments beyond 90 days, poor credit rating, etc. The screening will be conducted by a Credit Bureau and is based on name, birth date and Social Insurance Number (SIN). Details of an applicant's credit information are **not** disclosed.

Enhanced Security Screening: involves a Criminal Records Check, Financial Management Risk Indicator Screening and the verification of applicant's loyalty (Vulnerability Risk Indicator Screening) as it relates to the security of Canada as defined in Section 2 of the Canadian Security Intelligence Service (CSIS) Act. CSIS screens applicant's information against the CSIS data for the following issues:

- Espionage or sabotage
- Foreign influenced activities

- Threat or use of serious violence to achieve a political, religious or ideological objective
- Political violence leading to the destruction of the established system of the government of Canada.

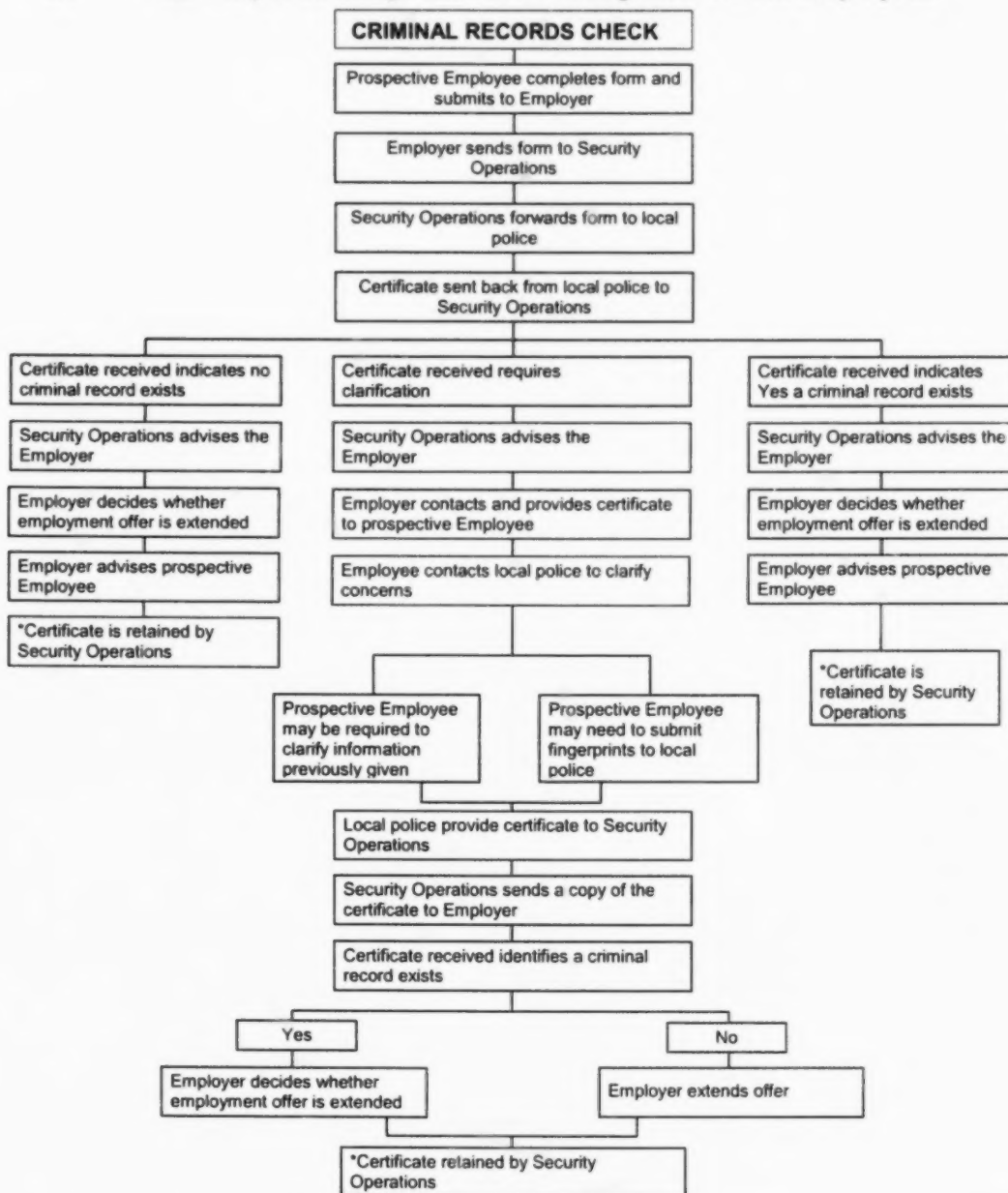
About this Directive

Authority: Public Service Act

Application: Organizations under the *Public Service Act*

Effective Date: 1 February 2003

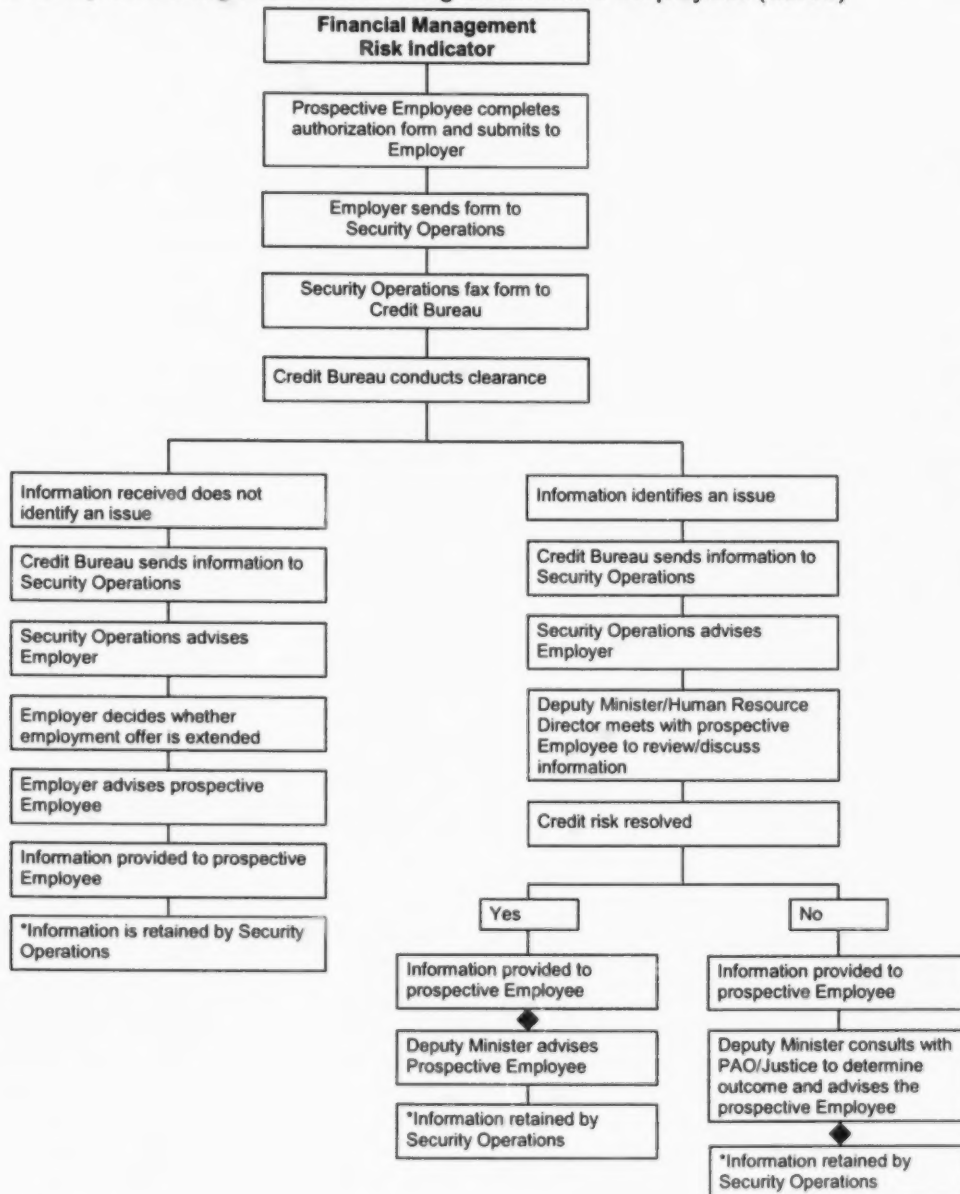
Contact: Staffing
Executive Search

6.0 APPENDIX 2**6.1 Security Screening Process for Designated Future Employees**

* Information retained by Security Operations is accessible to the prospective employee and/or the Ministry's Deputy Minister.

Note: Employer – refers to Executive Search for recruitment/exemptions of Executive/Senior Official positions noted on the Security Screening Directive.
For other positions in the Public Service – Employer refers to Human Resources

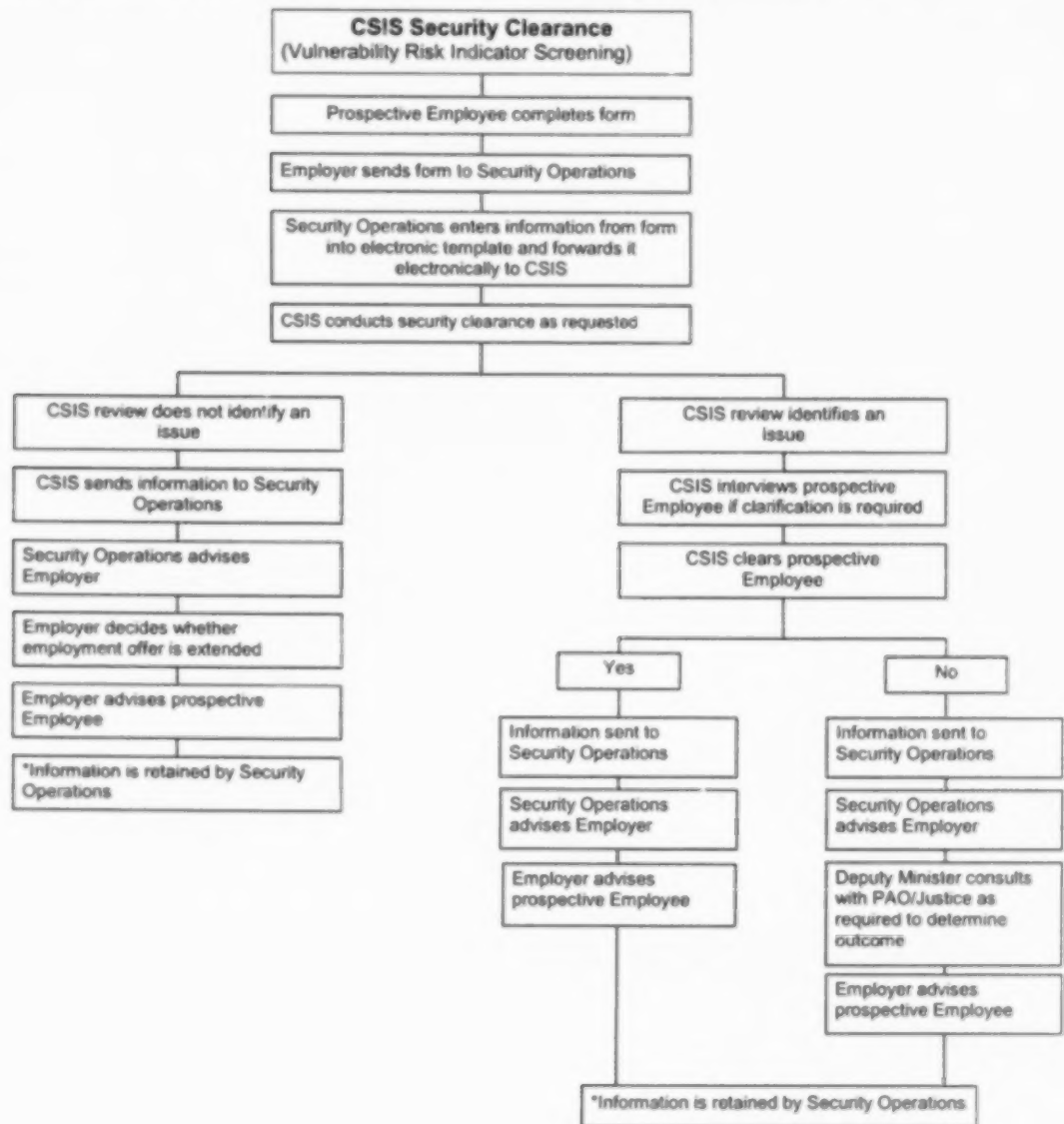
Security Screening Process for Designated Future Employees (cont'd)



* Information retained by Security Operations is accessible to the prospective employee and/or the Ministry's Deputy Minister.

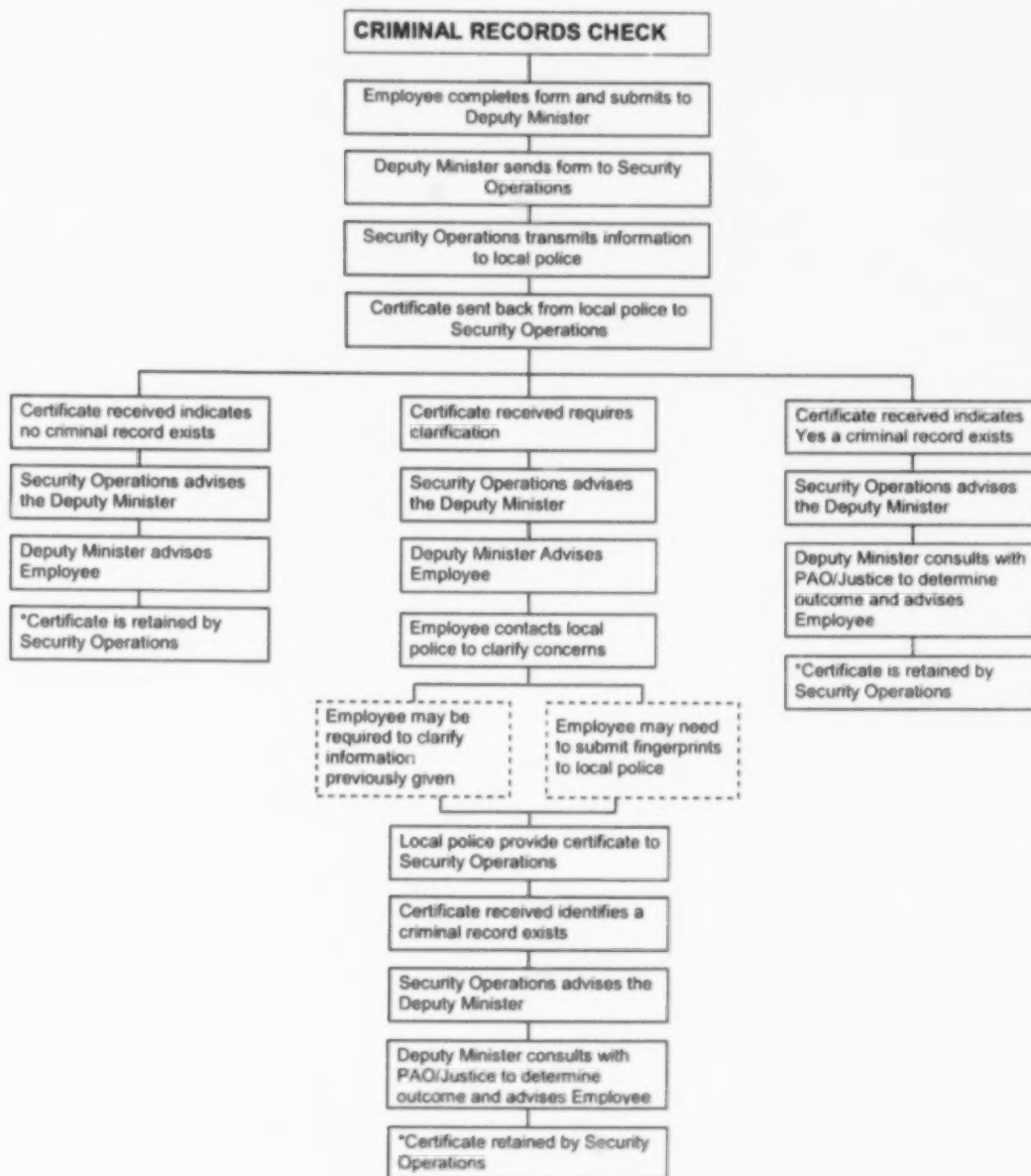
Note: *Employer* – refers to Executive Search for recruitment/exemptions of Executive/Senior Official positions noted on the Security Screening Directive.
For other positions in the Public Service – Employer refers to Human Resources.

Security Screening Process for Designated Future Employees (cont'd)



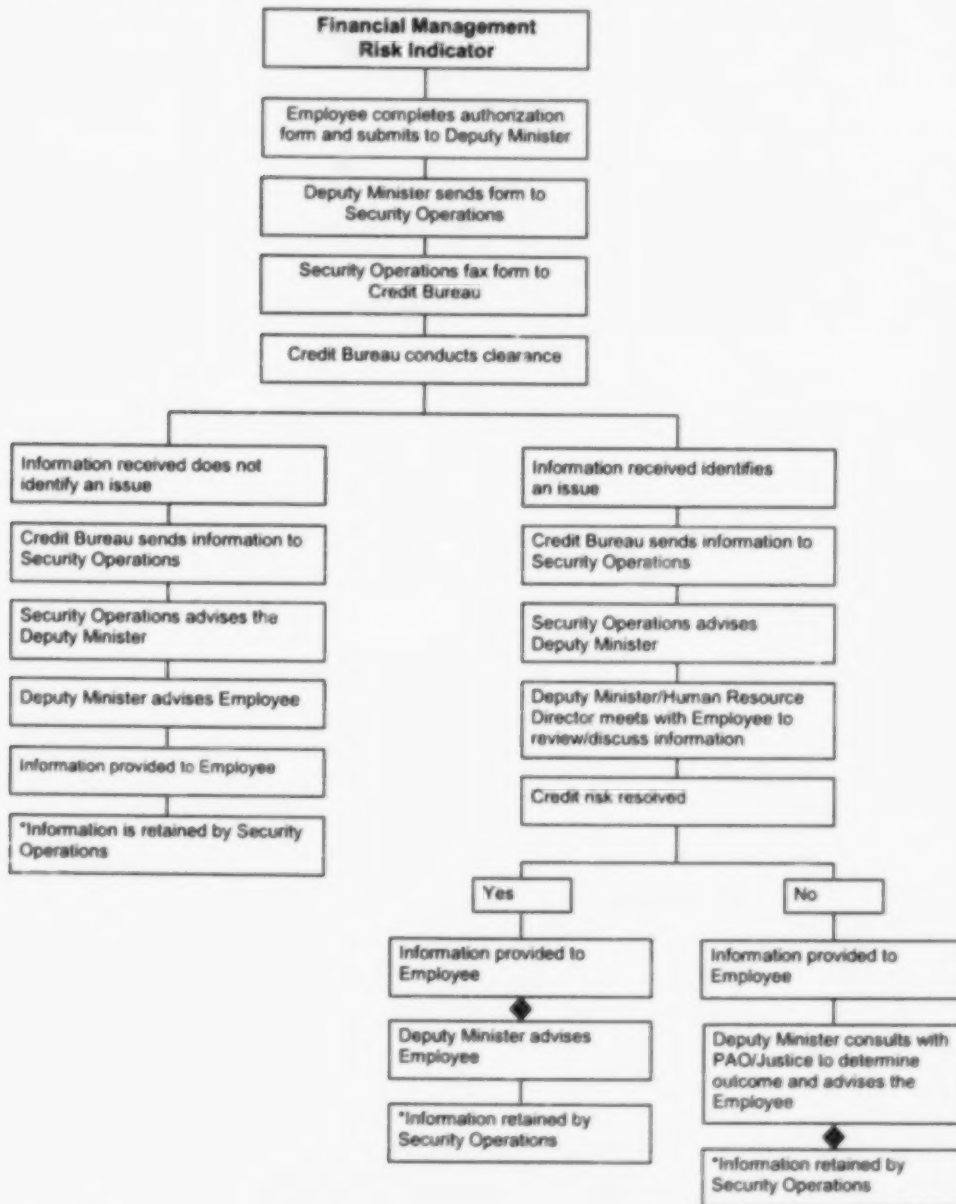
* Information retained by Security Operations is accessible to the prospective employee and/or the Ministry's Deputy Minister.

Note: Employer – refers to Executive Search for recruitment/exemptions of Executive/Senior Official positions noted on the Security Screening Directive.
For other positions in the Public Service – Employer refers to Human Resources.

6.2 Security Screening Process for Designated Current Employees

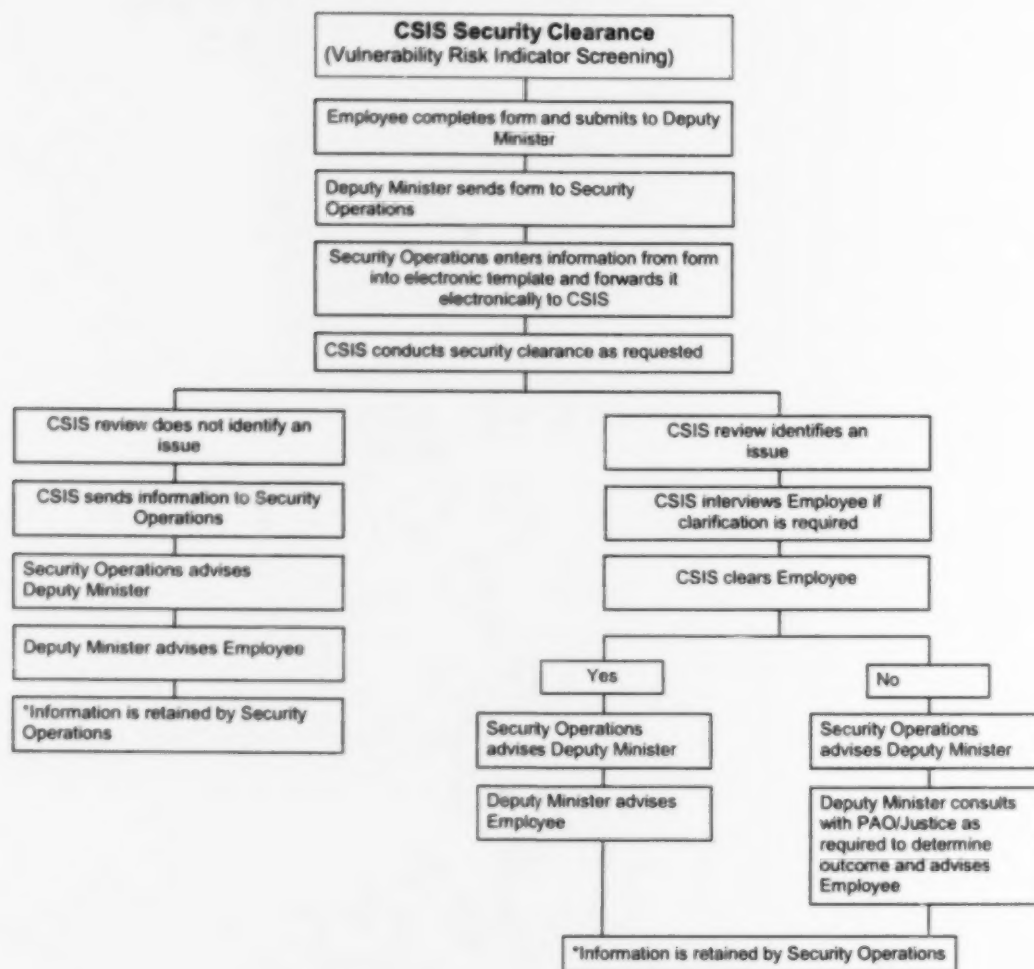
* Information retained by Security Operations is accessible to the Employee and/or their Deputy Minister.

Security Clearance Process For Designated Current Employees (continued)



* Information retained by Security Operations is accessible to the employee and/or the Ministry's Deputy Minister.

Security Screening Process for Designated Current Employees (continued)



* Information retained by Security Operations is accessible to the Employee and/or their Deputy Minister.

7.0 APPENDIX 3

Applicant Security Screening Information (Instruction Sheet)

Consent Forms

Checklist Form

7.1 INSTRUCTION SHEET FOR CURRENT EMPLOYEES

In relation to the definitions outlined on the Alberta Security Screening Directive, the following steps will outline the process in completing the forms.

Forms completed are on a voluntary basis. If you choose not to complete the forms, the package may be returned or destroyed.

Forms completed must be returned to Security Operations, Solicitor General. It is recommended that Ministries return the forms for the Deputy Minister and all Executive Committee Members as a package. Security Operations upon receipt of the forms will forward the forms to the local police, the credit bureau and CSIS. They will receive the information from the appropriate agency and will advise the applicable Deputy Minister.

1. **Consent to Release Information Form:** Must be completed by the individual and is used to disclose the information by the employer to Security Operations.
2. **Criminal Records Check:** Involves a screening against the Canadian Police Information Centre (CPIC), based on name and birth date and is conducted by the applicable police force.

- The Security Clearance Check Form must be completed by the individual.
- Personal information must be fully completed.
- The section entitled Verification of Applicant's Identification must be completed by a supervisor or colleague. The person verifying the identification must print their name and sign the form and provide their phone number in the spaces provided. They must also check off which types of identification were presented to them (minimum 2).
- The Vulnerable Sector section need only be filled out and signed if applicable and desired by the Ministry.
- The waiver on the back of the form must be completed, signed and witnessed.

NOTE: Individual payment is not required. All billing will be managed through Security Operations.

3. **Financial Management Risk Indicator Screening:** Involves a screening for the presence of credit risk indicators such as bankruptcies, garnishees, credit payments beyond 90 days, poor credit ratings, etc. The screening will be conducted by a Credit Bureau and is based on name, birth date and Social Insurance Number. Details of an applicant's credit information are not disclosed.
 - The TransUnion Credit Form must be completed by the individual.
4. **Enhanced Security Screening:** Involves a Criminal Records Check, Financial Management Risk Indicator Screening and the verification of applicant's loyalty as it relates to the security of Canada as defined in Section 2 of the Canadian Security Intelligence Service (CSIS) Act. CSIS screens applicant's information against the CSIS data.
 - Complete the form with the exception of Sections M and N.

(Prospective Employees)**7.2 Sample Release of Information Consent Form****CONSENT TO RELEASE INFORMATION**

I, _____, authorize _____ to collect
(name of individual) (name of organization)
and release the results of the Security Screening they conducted, to Security
Operations, on behalf of _____, Government of Alberta.

The following screening will be conducted:

- | | |
|--|--------------------------|
| ☐ Criminal Records Check | _____ Applicant initials |
| ☐ Financial Management Risk Indicator | _____ Applicant initials |
| ☐ Enhanced Security Screening | _____ Applicant initials |
- (which includes a Criminal Records Check, Financial Management Risk
• Indicator and Vulnerability Risk Indicator Screening through Canadian
Security Intelligent Service (CSIS)).

These results are to be used only for the purpose of addressing the screening
criteria as established in the Alberta Security Screening Directive, and only as a
requirement for the position for which I am being considered. The information
from the screening will be shared with _____, who is charged
with responsibility of reviewing it for the purpose of this competition.

Collection, use, disclosure, security and retention of information are subject to
the *Freedom of Information and Protection of Privacy Act*.

Applicant Signature

Date

Witness Signature

Date

Witness Name

(Current Employees)**7.3 Sample Release of Information Consent Form****CONSENT TO RELEASE INFORMATION**

I, _____, authorize _____ to collect
(name of individual) (name of organization)
and release the results of the Security Screening they conducted, to Security
Operations, on behalf of _____, Government of Alberta.

The following screening will be conducted:

- | | |
|--|-------------------------|
| ☐ Criminal Records Check | _____ Employee initials |
| ☐ Financial Management Risk Indicator | _____ Employee initials |
| ☐ Enhanced Security Screening | _____ Employee initials |
- (which includes a Criminal Records Check, Financial Management Risk
• Indicator and Vulnerability Risk Indicator Screening through Canadian
Security Intelligent Service (CSIS)).

These results are to be used only for the purpose of addressing the screening
criteria as established in the Alberta Security Screening Directive. The
information from the screening will be shared with _____, who
is charged with responsibility of reviewing it for the purpose of their management
or advisory responsibilities within the Alberta Public Service.

Collection, use, disclosure, security and retention of information are subject to
the *Freedom of Information and Protection of Privacy Act*.

Employee Signature

Date

Witness Signature

Date

Witness Name

ALBERTA

7.4 Checklist Form

Name of Candidate/Employee _____

Please fill in the appropriate information which reflects one of the following transactions:

Competition No.: _____

Exemption No.: _____

Reclassification/Position No.: _____

An X is placed beside the appropriate security screening check(s) which will indicate the screening was completed.

____ Criminal Records Check	____ Completed	____ Date
____ Financial Management Risk Indicator Screening	____ Completed	____ Date
____ Vulnerability Risk Indicator Screening	____ Completed	____ Date

Signature of Human Resource Consultant/Human Resource Advisor

NOTE: This form is to be placed on the competition file or the personal file. The original copies of the security screening are maintained by Security Operations, Solicitor General.

8.0 APPENDIX 4

8.1 Edmonton Police Service Security Screening Check

(Insert sample here)

9.0 APPENDIX 5**9.1 Alberta Financial Risk Management Indicator Screening****PLEASE PRINT CLEARLY**

Name(s) include name changes, maiden name, etc.

Surname

First Name

Middle Name

Previous Surname

Address

Postal Code

Birthdate

Gender

Year Month Day

____ Male ____ Female

I hereby consent to and authorize the _____
(name of organization)
to undertake a credit screening to request and obtain personal information about me
from credit bureaus from information they previously collected about me in order to
assess my credit history.

I further authorize the _____ (name of organization)

_____ to destroy the relevant information once obtained and reviewed within 3
(three) weeks of receipt of the information, or

_____ to send the credit information to my home address.

Signature of Applicant/Employee

Date

Authorized Department Representative

PIA – Final Report

9.2 Financial Management Risk Indicator Report Form**Alberta Public Service
Financial Risk Management Indicator Form****Alberta Provincial Government
Employee Information**

Employee Name: _____

Items on credit report:	Yes	No
1. Bad Debt write offs		
2. Paid Collections		
3. Unpaid Collections		
4. Bankruptcies		
5. Discharged from Bankruptcy (not applicable, leave blank)		
6. ABM or Bank Frauds		
7. Active Judgments		
8. Paid Judgments		
9. Ratings above R2 (Revolving Credit) or I2 (Installment Credit)		
10. NSF Cheques		

Yes to any of these items indicates one or more of these will be on the individual's credit file.

10.0 APPENDIX 6

10.1 Alberta Enhanced Security Screening Instructions

10.2 Alberta Enhanced Security Screening Form

Please note: the following documents are on a legal sized (14") format

General:

- If clarification of information is required, a Canadian Government Official may contact the applicant to obtain additional information in order to complete the security screening investigation and an interview of the applicant may be requested.
- This form is to be completed using an automated system or if not available using a typewriter or printing in block letter format in black ink.
- Please read and follow these instructions carefully.
- The original signed copy must be submitted.
- It is important that a copy of the completed questionnaire be retained by the applicant for future reference.
- Incomplete or illegible forms will NOT be considered.
- All names are to be in full (no initials) (Maternal and Paternal or other names used).
- Addresses are to include, where applicable, civic or township name and the lot and concession numbers.
- If information is not known or is unavailable please indicate this on the form and on a separate sheet of paper explain the cause of circumstance.
- All dates are to be entered in order of YEAR, MONTH, and DAY as applicable.
- If space allotted in any portion is insufficient, please use separate sheet using same format.

Detailed Instructions:

10.3 SECTION A

- To be completed by the Ministry Human Resources.

(Remainder of the form is to be completed by the applicant)

SECTION B

- Complete as requested.

10.4 SECTION C

- Complete as requested.

10.5 SECTION D

"Common-law partner" – In relation to an applicant, means a person who is cohabiting with the individual in a conjugal relationship, having so cohabited for a period of at least one year. This includes persons of the same sex.

- 1. Includes current spouse and common-law partner as applicable.
- If any person is deceased, date of death and last address while living are to be shown.
- 2. Includes previous spouse and common-law partner as applicable during the last five years.
- If a person is deceased, date of death is to be shown in 2e.
- All other questions to be answered as set forth.

10.6 SECTION E

- List only criminal convictions for which a pardon has NOT been granted. Include on a separate attached sheet of paper, if more than one conviction. Applicant must include those convictions outside Canada.
- Offences under the *National Defence Act* are to be included as well as convictions by courts-martial are to be recorded.

10.7 SECTION F

- If a naturalized Canadian, it is important to show the certificate number, date of issue. Attach a photocopy of the certificate.
- If born abroad of Canadian parents, please provide a copy of your Certificate of Registration of Birth Abroad.
- If not a Canadian Citizen indicate if application has been made for Citizenship. In this case, passport or identify card number and particulars should be recorded in box "6". Please provide copy of Immigrant Visa or Record of Landing documentation.
- Questions 5 and 6 – Attach a separate sheet of paper if more space is required. Each sheet must be signed.

10.8 SECTION G

- As set forth, ensuring current address is recorded first.
- The Postal Code is mandatory for the current address, and if known, for previous addresses.
- For rural area, include civic number or lot, concession and township number.

SECTION H

- Record your present employment first. If you have held a number of different positions within the same Ministry, do not list them. You should only indicate your current position but reflect the date of when you originally commenced with the Ministry. If you have worked in other Ministries, indicate the last position held but reflect the date of when you originally commenced with the Ministry.
- Please note that it may be necessary to contact your present employer.
- Time at school and periods of unemployment are also to be shown; (as well as, secondments, educational leave, and courses of over six months' duration; include supervisor or colleague's name).
- Job-site address is the address where your work is performed and may be different from your employer's address.

ALBERTA ENHANCED SECURITY SCREENING FORM

Note: If you are self-employed or a consultant, or have been self-employed or a consultant, provide the following:

- a) Name of employer – give your business name; if not applicant, give your name;
- b) No change;
- c) Job-site address – give your permanent business address; if not applicable, give your residence address;
- d) No change;
- e) No change;
- f) Supervisor's name – give a name of a person who can verify your employment;
- g) No change.

10.9 SECTION I

- Is related to determining past employment of security concern. A security official may ask for further details.

10.10 SECTION J

- Complete as requested.

10.11 SECTION K

- Complete as requested.

10.12 SECTION L

- Applicant check off numbers 1 through 4 and initials each section under the column titled, "Applicant's Initials".
- The balance of this section will be completed by Security Operations.

10.13 SECTIONS M/N (do not complete these two sections)

- To be completed by Security Operations.

10.14 SUPPLEMENTAL INFORMATION REQUIREMENTS

Persons who have previously completed a SECURITY CLEARANCE and subsequently marry, remarry or commence a common-law partnership are required to submit an original Security Clearance Form with the following parts completed:

For all Security Clearances

- Part A-D – As set forth in each question
- Part K-L – To be signed by person submitting the form

Note: In addition to the above, in those cases where an individual marries or commences a common-law partnership with a Non-Canadian National or Landed Immigrant who has not yet arrived in Canada, the following information is required:

- Parts A-D – As set forth in each question
- Part G – For new spouse/common-law partnership
- Part H – For new spouse/common-law partnership
- Part K-L – To be signed by person submitting the form

Please forward the completed and signed Alberta Security Screening Form to your ministry Human Resources.

Human Resources to forward the Alberta Security Screening Form to:

Public Security Division
Security Operations Branch
Solicitor General
Pedway Mall, Government Centre
10820 – 98 Avenue
Edmonton, Alberta T5K 2N6

ALBERTA ENHANCED SECURITY SCREENING FORM

A ADMINISTRATIVE INFORMATION (To be completed by the Authorized Representative/Agency/Organization)			
☒ New	☐ Upgrade	☐ Supplemental	Level II Enhanced Security Screening
☐ Update	☐ Transfer	☐ Re-activation	
PARTICULARS OF APPOINTMENT/ASSIGNMENT/CONTRACT			
Position/Competition/Contract number		Title	
Employee ID number (if applicable)	If term or contract, indicate duration period	From	To
Name and address of department/organization/agency Government of Alberta		Name of official	Telephone number () ()
			Facsimile number () ()
B BIOGRAPHICAL INFORMATION (To be completed by the applicant)			
1. Surname (last name)		2. Full given names (no initials) underline or circle usual name used	
		3. Family name at birth	
4. All other names used (i.e. nickname)		5. Sex ☐ Male ☐ Female	6. Date of birth YYYY MM DD
7. Place of birth (city)	Province/State	Country	
8. Name change (other than marriage)	From	To	
9. Place of change (city, province or state and country)		10. Method (authority)	
C SECURITY SCREENING			
1. Have you previously completed a Government of Canada security screening form? ☐ Yes ☐ No			
If yes, give name of employer, level and year of screening YYYY			
D MARITAL STATUS/COMMON-LAW PARTNERSHIP			
CURRENT STATUS			
☐ Married ☐ Common-Law Partnership ☐ Separated ☐ Widowed ☐ Divorced ☐ Single			
A) CURRENT SPOUSE/COMMON-LAW PARTNER Surname, given names		B) Maiden Name (if applicable)	
C) Present citizenship of current spouse/common-law partner			
D) Date of marriage/common-law partnership YYYY MM DD		E) City, province or state, and country of marriage/common-law partnership	
F) City, province or state, and country of birth		G) Date of birth YYYY MM DD	
H) Present address (apartment number, street number, street name, civic number (if applicable), city, province or state, and country)		I) If separated, widowed or divorced, specify date YYYY MM DD	
J) Name and address of employer (job title)			
2 PREVIOUS SPOUSE/COMMON-LAW PARTNER			
A) PREVIOUS SPOUSE/COMMON-LAW PARTNER: Surname, given names (cover only the past five years)		B) Present citizenship of former spouse/common-law partner	
C) Date of marriage/common-law partnership YYYY MM DD		D) City, province or state, and country of marriage/common-law partnership	
E) Date of divorce/separation/deceased YYYY MM DD		F) City, province or state, and country of divorce	
G) Country of Birth (if known)		H) Date of Birth YYYY MM DD	

ALBERTA ENHANCED SECURITY SCREENING FORM

Surname	Date of Birth
	YYYY MM DD

E CRIMINAL CONVICTIONS IN AND OUTSIDE OF CANADA (see instructions)

Have you ever been convicted of a criminal offence for which you have not been granted a pardon?

☐ Yes☐ No

If yes, give details (charge(s), name of police force, city, province/state, country and date of conviction)

Charge(s)	Name of police force	City
Province/State	Country	Date of conviction
		YYYY MM DD

F FOR COMPLETION BY PERSONS BORN OUTSIDE CANADA OR BORN IN CANADA HOLDING DUAL

1. Date of entry into Canada	2. Present citizenship
YYYY MM DD	
3. If you are a naturalized Canadian, give the certificate number and date of issue	4. If you are not naturalized, have you applied for Canadian citizenship?
Certificate No. YYYY MM DD	☐ Yes ☐ No
	Date of application YYYY MM DD
5. Do you maintain citizenship of a country other than Canada?	6. Have you used a passport other than a Canadian one? If yes, explain why.
☐ Yes ☐ No	☐ Yes ☐ No
(If yes) Name of Country	(If yes) Explain:
Explain:	

G RESIDENCE (there should be no gaps)

List addresses where you have lived during the last 10 years, starting with the most current. (Rural address to include lot and civic number.)

	Apartment #	Street #	Street name	Civic number (if applicable)	From	To	To present
1					YYYY	MM	Telephone number ()
	City		Province or State	Postal Code	Country		
2					YYYY	MM	Telephone number ()
	City		Province or State	Postal Code	Country		
3					YYYY	MM	Telephone number ()
	City		Province or State	Postal Code	Country		
4					YYYY	MM	Telephone number ()
	City		Province or State	Postal Code	Country		
5					YYYY	MM	Telephone number ()
	City		Province or State	Postal Code	Country		

H EMPLOYMENT (last 10 years) (see instructions for self-employed and consultants) (there should be no gaps)

Would your employment be jeopardized if your current supervisor, below, is contacted?

☐ Yes☐ No

If yes, provide the name of an alternate employment contact and telephone number

Were you dismissed or asked to resign from any position(s) as listed below?

☐ Yes☐ No

If yes, give name of employer, supervisor, and date

Name of employer	Supervisor	Position Title	Date
			YYYY MM DD

ALBERTA ENHANCED SECURITY SCREENING FORM

Surname		Date of Birth		YYYY	MM	DD
A) Name of employer - do not use initials (department/organization/agency, if applicable)		B) From To YYYY MM Present				
C) Job-site address (street number, street name, city, province or state, and country)						
1	D) Job title/Description		E) Rank and service number (if applicable)			
	F) Supervisor's name in full		G) Supervisor's telephone number ()			
A) Name of employer - do not use initials (department/organization/agency, if applicable)		B) From To YYYY MM YYYY MM				
C) Job-site address (street number, street name, city, province or state, and country)						
2	D) Job title/Description		E) Rank and service number (if applicable)			
	F) Supervisor's name in full		G) Supervisor's telephone number ()			
A) Name of employer - do not use initials (department/organization/agency, if applicable)		B) From To YYYY MM YYYY MM				
C) Job-site address (street number, street name, city, province or state, and country)						
3	D) Job title/Description		E) Rank and service number (if applicable)			
	F) Supervisor's name in full		G) Supervisor's telephone number ()			
A) Name of employer - do not use initials (department/organization/agency, if applicable)		B) From To YYYY MM YYYY MM				
C) Job-site address (street number, street name, city, province or state, and country)						
4	D) Job title/Description		E) Rank and service number (if applicable)			
	F) Supervisor's name in full		G) Supervisor's telephone number ()			
I FOREIGN EMPLOYMENT						
1. Are you now or have you ~~you~~ been employed by or acted as a consultant for a foreign government, firm, or agency? ☐ Yes ☐ No		If yes, give details (country, organization, nature of work and dates) include military (cadets), law enforcement and security intelligence employment. 				
J EDUCATION						
1. Name of the last school or university where attended full time		2. Student ID number (if known)		3. Location of institution		
5. Field of study (diploma or degree obtained)		4. Period of attendance From To YYYY MM YYYY MM				
K CERTIFICATION						
I hereby certify that the information set out by me in this document is true and correct to the best of my knowledge and belief.						
1. Signature		2. Date YYYY MM DD		3. Telephone (home) ()		4. Telephone (business) ()

Surname	Date of Birth	YYYY	MM	DD
---------	---------------	------	----	----

I. CONSENT AND VERIFICATION To be completed by the applicant and authorized Departmental Agency Organizational Official.

Information (see instructions)	Applicant's initials	Name of official (print)	Official's initials	Official's Telephone number
1. ☐ Date of birth, address, education, professional qualifications, employment history, personal character references.				()
2. ☐ Criminal record check.				()
3. ☐ Credit check (financial assessment, including credit records check).				()
4. ☐ Loyalty (security assessment only)				
5. ☐ Other (specify, see instructions)				()

The information on this form is required for the purpose of providing security screening assessments. It is collected under the authority and the provisions of the Freedom of Information and Protection of Privacy Act.

I, the undersigned, do consent to the disclosure of the preceding information and its subsequent verification to the Government of Canada, the use of my photograph for identification purposes and the release of a copy of Section L of this form, if required.

Signature Date (yyyy/mm/dd)

The Security Assessment conducted by C.S.I.S. operate under federal legislation. In order for C.S.I.S. to conduct the checks, the information will be disclosed to Security Operations, Solicitor General. The information from the security assessment will be reported to the Deputy Minister and may be disclosed to the Deputy Minister of Executive Council and legal or human resource advisors as required who are charged with the responsibility of reviewing it for the purpose of their management or advisory responsibilities within the Alberta Public Service.

II. REVIEW To be completed by the authorized Departmental Agency Organizational Official responsible for ensuring the completion of sections I and II.

Name and Title	TELEPHONE NUMBER
	()
Address	Facsimile number
	()

III. APPROVAL To be completed by authorized Departmental Agency Organizational Security Official only.

I, the undersigned, as the authorized security official, do hereby approve the following level of screening:

☐ Enhanced Security Screening ☐ Not Approved

Name and Title

Signature Date (yyyy/mm/dd)

ALL INFORMATION SUPPLIED IS SUBJECT TO VERIFICATION BY INVESTIGATION.